العنوان:	التحقيق في جرائم تقنية المعلومات
المصدر:	مجلة الفكر الشرطي - مركز بحوث الشرطة - القيادة العامة لشرطة الشارقة - الإمارات
المؤلف الرئيسي:	المعيني، سرحان حسن
المجلد/العدد:	مج20, ع79
محكمة:	نعم
التاريخ الميلادي:	2011
الشهر:	أكتوبر
الصفحات:	15 - 54
رقم MD:	605735
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	تقنية المعلومات
رابط:	http://search.mandumah.com/Record/605735

التحقيق في جرائم تقنية المعلومات [1]

المقدم الدكتور سرحان حسن المعيني [2]
أستاذ علوم الشرطة المساعد - أكاديمية العلوم الشرطية بالشارقة - الإمارات

مستخلص

لا شك أن المجتمع الدولي يمر في الوقت الراهن بثورة هائلة من التحولات بما يعرف اصطلاحاً بظاهرة العولمة ، والتي أفرزت حالة من التواصل الإنساني بفضل الثورة المعلوماتية وتقنياتها. وقد تزامن الحديث عن جرائم تقنية المعلومات في الفترة الحديثة مع بروز مجموعة من الظواهر الحياتية والمستجدات الفكرية والتطورات التكنولوجية والعلمية التي تتجه نحو زيادة ترابط العالم وتقاربه ، مما أدى إلى إلغاء الحدود والفواصل بين الأفراد والمجتمعات والثقافات والدول. كما يشهد العالم تغيرات هامة جداً في الثورة التكنولوجية والمعلوماتية وأصبح محاطاً بأنماط وصور من الجرائم المستحدثة وغيرها من أشكال جرائم تقنية المعلومات الخطيرة ، حيث تشكل هذه الجرائم حيثما وجدت خطراً يهدد الحفاظ على سيادة القانون في معظم الدول نظراً لكونها جرائم في معظم الأحوال ذات أبعاد دولية. لذا تسعى هذه الدراسة بصفة أساسية إلى محاولة استكشاف وتحديد معالم إحدى صور الظاهرة الإجرامية المستحدثة التي ترتكب بواسطة تقنية المعلومات من حيث تعريفها وتحديد أهم أنماطها وصورها ، وضرورة تحديد الإجراءات الواجب اتباعها في ضبط وتحقيق جرائم تقنية المعلومات وتقنية التحفظ على الأجهزة المستخدمة في ارتكاب هذه الجرائم وكيفية مقارنتها . وقد انطلقت الدراسة من فرضية الكفاءة والفاعلية في أنشطة مكافحة جرائم تقنية المعلومات واعتمدت الدراسة على المنهج التحليلي التطبيقي واشتملت على عدة محاور رئيسية هي الأبعاد المختلفة لجرائم تقنية المعلومات وسماتها وخصائصها والمخاطر التي تطرحها والمشكلات العلمية والعملية في تحقيق جرائم تقنية المعلومات وصعوبات وإشكاليات هذه الجرائم وما هي الأصول الفنية الواجب مراعاتها في الانتقال والمعاينة والتفتيش عندما يتعلق الأمر بجريمة معلوماتية ، وقد انتهت الدراسة إلى أن المشكلات المثارة من خلال مكافحة جرائم تقنية المعلومات لم نجد لها حلاً في القريب العاجل والمسائل المستقبلية التي ينبغي توجيه النظر إليها هي تلك المتعلقة بالتحليل العلمي لإساءة استخدام تكنولوجيا تقنية المعلومات والإنترنت ومكافحته ولذلك فإن الدراسة أوصت بأن يتدخل المشرع الإماراتي ببعض التعديلات الإجرائية المتعلقة بجرائم تقنية المعلومات حيث أن النصوص الإجرائية الجزائية باتت غير ملائمة للتطبيق على جرائم تقنية المعلومات كما أن الدراسة تأمل أن يتبنى الفقه والقضاء تفسيراً متطوراً للنصوص العقابية المتعلقة بجرائم تقنية المعلومات في إطار من الشرعية الجنائية.

مفردات البحث :

تقنية المعلومات — الجريمة المعلوماتية — المجرم المعلوماتي — المعاينة — التفتيش — الأدلة الجنائية — الدليل التقني — التحقيق المعلوماتي .

1- ورد هذا البحث للدورية في يونيو 2011م وأحيل للتحكيم في يوليو 2011م وأجيز للنشر في سبتمبر 2011م.

2- حصل المقدم الدكتور. سرحان حسن المعيني على درجة الدكتوراه في علوم الشرطة عام 2005م ، ويشغل حالياً منصب مدير أكاديمية العلوم الشرطية بالشارقة بالإمارات ويرأس العديد من اللجان بالأكاديمية ، وله العديد من البحوث والدراسات الأكاديمية ومشارك في مؤتمرات وندوات محلية ودولية.

مقدمة :

الجريمة ظاهرة اجتماعية ، على هذا اتفق علماء الإجرام ، تتأثر حجما واتجاها وصوراً وأنماطا بالمتغيرات المجتمعية المختلفة على كافة مستوياتها الاقتصادية والاجتماعية والثقافية.

ولا شك أن المجتمع الدولي يمر في الوقت الراهن بثورة هائلة من التحولات بما يعرف اصطلاحاً بظاهرة العولمة ، والتي أفرزت حالة من التواصل الإنساني بفضل الثورة المعلوماتية وتقنياتها والتي عكست بدورها انساقاً قيمية وثقافية ذات مردودات سلبية صاحبها ظهور أنماط إجرامية مستحدثة اتخذت من تقنية المعلومات الهائلة أداة ووسيلة ومحلاً للاعتداء على مجموعه من المصالح والقيم الاجتماعية والشخصية الأساسية [1].

وقد تزامن الحديث عن جرائم تقنية المعلومات في الفترة الحديثة مع بروز مجموعة من الظواهر الحياتية والمستجدات الفكرية والتطورات التكنولوجية والعلمية التي تتجه نحو زيادة ترابط العالم وتقاربه ، مما أدى إلى إلغاء الحدود والفواصل بين الأفراد والمجتمعات والثقافات والدول.

وهكذا تساندت وتجمعت مجموعة من المعطيات التي ولدتها التحولات والتغيرات العالمية لتفرز هذا النمط المستحدث من جرائم تقنية المعلومات ولتضيف للبشرية هموما جديدة. فقد ظهر ما يسمى بالحاسوب ، وبدأ يغزو الحياة تدريجياً ، وفي تطور متزايد ، أدى إلى اتساع جوانب الاستعانة به في كثير من المجلات ، كالصناعة ، والتجارة ، والنقل ، والطب ، والدفاع ، والتعليم ، والبحوث ، مما كان يلزم معه ضرورة توفير الحماية اللازمة لهذه الأجهزة والمعلومات التي تحملها [2].

1- د. أحمد وهدان ، الانعكاسات الأمنية للعولمة ، القاهرة : المجلة الجنائية القومية ، مج 44 ، ع1 ، 2 ، مارس/يوليو 2001 ، ص91.

2- راجع في ذلك الدكتور/ حسني الجندي : التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة ، الكتاب الثالث. قانون مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة : الطبعة الأولى سنة 2009م ، ص3 وما بعدها.

واتبع ذلك ظهور الانترنت أو ما يطلق عليه الشبكة المعلوماتية أو شبكة الشبكات ، والذي أصبح أداة التواصل بين شبكات المعلومات ، بهدف تبادل المعلومات ، واتسم بأنـــه عابر للحدود الدولية (1).

وكان نتيجة تزايد أهمية استخدام وسائل تقنية المعلومات وكثرة الاعتماد على الحاسوب، وشبكات المعلومات ، وفي مقدمتها الانترنت ، أن ظهر في السنوات الأخيرة أشكال جديدة مـــن الجرائم تستهدف المعلومات وبرامج الحاسوب ، كالدخول غير المصرح به إلى أنظمة الحاسوب والشبكات ، والاستيلاء على المعلومات أو إتلافها عبر تقنيات الفيروسات وغيرها من وســائل التدمير المعلوماتي ، وجرائم قرصنة البرمجيات والاعتداء على حقوق الملكية الفكرية لمؤلفيها وجهات إنتاج هذه البرامج.

وشاعت أيضاً الجرائم التي تستخدم الحاسوب وشبكة المعلومات كوســيلة لارتكـــاب أنشطة إجرامية تقليدية ، كالاحتيال عبر الحاسوب ، والتزوير باستخدام التقنيات الحديثـــة. هذا عوضاً عن طائفة جديدة من الجرائم استخدمت تكنولوجيا المعلومات كبيئة لها ، كما في جرائم توزيع المحتوى غير القانوني عبر مواقع الانترنت ، وجرائم المقـــامرة والأنشـــطة الإباحية عبر الانترنت ، أو استثمار مواقع الانترنت كمخازن للبيانات الإجرامية ومواضـــع لتنسيق أنشطة الجريمة المنظمة وجرائم غسل الأموال الالكترونية.

ونظراً لخطورة جرائم تقنية المعلومات ، فقد أصدر المشرع الإماراتي القانون رقـــم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات. والذي يبين من مطالعة نصوصه

1- راجع في هذا المعنى. عمر محمد أبوبكر بن يونس. الجرائم الناشئة عن استخدام الانترنت ، رسالة عين شمس سنة 2004م ، ص31- المستشار محمد احمد الحمادي: تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات ، أحكام القضاء ، ضمن مجموعة البحوث الخاصة بالندوة العلمية التي نظمها مركـــز البحوث والدراسات الأمنية ، القيادة العامة لشرطة أبوظبي في الفترة من 6-7 نـــوفمبر ســـنة 2006م ، ص9 وما بعدها.

التي بلغت (29) مادة أنه ذا طابع موضوعي ، وأن مادة واحدة فقط منها يتعلــق بالأحكــام الإجرائية. وصنف المشرع الجرائم المعلوماتية في (23) مادة وهي المواد من (2) حتــى (23). وخصص المواد من (24) حتى (26) للعقوبات المقررة لتلك الجرائم. ولــم يفــرد المشرع إلا نصاً واحداً للأحكام الإجرائية هي المادة (27) منه ، وإن كانت واسعة النطاق ، إذ تشمل تحديد مأموري الضبط القضائي المكلفين بضبط الجرائم التي تقع بالمخالفة لأحكام هذا القانون ، وتبعيتهم ، وسلطاتهم ، ومراحل الدعوى الجزائية في جرائم تقنية المعلومات.

أهمية الدراسة :

يشهد العالم تغيرات هامة جدا في الثورة التكنولوجية والمعلوماتية وأصــبح محاطــاً بأنماط وصور من الجرائم المستحدثة وغيرها من أشكال جرائم تقنية المعلومات الخطيرة ، حيث تشكل هذه الجرائم حيثما وجدت خطراً يهدد الحفاظ على سيادة القانون فــي معظــم الدول نظراً لكونها جرائم في معظم الأحوال ذات أبعاد دولية وما يشكله ارتفــاع وزيــادة حجمها وتنوع صورها وأنماطها من مخاطر تهدد الأمن الفردي والجماعي لمختلف الــبلاد والشعوب.

وعلى هذا النحو تنبع أهمية هذا البحث من دور الثورة المعلوماتية في عملية التنمية الشاملة بنوعيها الاقتصادي والاجتماعي وحاجتها من ثم إلى بحث المشكلات القانونية بــه ومحاولة الوصول إلى إيجاد الحلول المناسبة لها.

ومن ناحية أخرى فان المعلوماتية باعتبارها ظاهرة إنسانية واقتصادية واجتماعية لا يمكن أن تتطور بذاتها دون أن تتوافر لها القواعد القانونية التي تنظم اســتغلالها ، ونظــرا لأنها في مرحلة التطور والتفاعل فإنها شأنها شأن أي تطور جديد تحمل في طياتها الجانب المظلم الذي يتجسد في مجال القانون الجنائي بظهور (المجــرم المعلومــاتي) (والجريمــة المعلوماتية) أو ظاهرة الإجرام المعلوماتي بصفة خاصة.

وأمام هذا الشكل الجديد من الإجرام لا يبدو قانون الإجراءات الجزائية في حالته الراهنة كافيا أو فاعلاً على النحو المطلوب أو المرضي فنصوصه والنظريات والمبادئ القانونية التـــي يتضمنها أو تقف وراءه موروث بعضها من القرن التاسع عشر ، وتطبيق بعضها على أشـــكال جديدة للجرائم تستعير من تقنيات الحاسبات الآلية والمعلومات أساليبها لا يصـــطدم بصـــعوبات ناجمة عن الطبيعة الخاصة والخصائص الفنية الفريدة للوسائل المعلوماتيـــة المســـتخدمة فـــي ارتكابها وإنما تعترضه كذلك صعوبات رئيسية أخرى مرجعها أن نصوص الملاحقة التقليديـــة كإجراءات الضبط والتحقيق في مثل هذه النوعية من الجرائم قد وضعت في ظل تفكير يقتصر إدراكه على الجرائم المادية والمستندات ذات الطبيعة المادية مما يتعذر معه تطبيقها لحماية القيم غير المادية المتولدة عن المعلوماتية وتقنية المعلومات.

وانطلاقاً من الأهمية البالغة لهذا الموضوع على نحو ما أوضحنا فيما تقدم ، تبين أن هناك حاجة ماسة للبحث المتعمق في المسائل العملية المتصلة بتحقيق وإثبات جرائم تقنيـــة المعلومات ، لذا فإن هذه الدراسة تنصب على سبر غور المســـائل الفنيـــة والقانونيـــة ذات الصلة بتحقيق وإثبات جرائم تقنية المعلومات. وتهدف إلى تحديد منضـــبط لأبـــرز صـــور جرائم تقنية المعلومات والإنترنت في ضوء ما وصلت إليه الدراسات الجنائية المتخصصـــة من تطور على مدى السنوات الأخيرة في هذا الحقل ، وتهدف إلى الوقوف على التحـــديات التي تواجه التحقيق في هذا النمط المستجد من الجرائم ، كما تسعى إلـــى بيـــان الأصـــول العلمية والعملية لإجراءات التحقيق في البيئة الرقمية.

أهداف الدراسة :

تسعى هذه الدراسة بصفة أساسية إلى محاولة استكشاف وتحديد معالم إحدى صـــور الظاهرة الإجرامية المستحدثة التي ترتكب بواسطة تقنية المعلومات مـــن حيـــث تعريفهـــا وتحديد أهم أنماطها وصورها والعوامل الفاعلة فيها والمخاطر والتهديدات التي تطرحها هذه النوعية من الجرائم وانعكاساتها ومردوداتها السلبية علـــى كافـــة القطاعـــات الاجتماعيـــة والاقتصادية والثقافية والأخلاقية ، ومعايير خصائصها وسماتها المميزة لهـــا عـــن بـــاقي

الجرائم التقليدية ، ثم تقييم فعاليات المواجهة التشريعية لها وخاصة من حيث إجراءات ملاحقتها سواء مرحلة جمع الاستدلالات أو مرحلة التحقيق الابتدائي وبيان صعوبات ومشكلات الإثبات الجنائي التي تواجه المحقق واستعراض مدى مشروعية الدليل المستمد من أجهزة التقنية الحديثة لملاحقة مرتكبيها وتقديمهم للعدالة والإثبات الجنائي في حقهم.

مشكلة الدراسة :

يتسم التحقيق في جرائم تقنية المعلومات والإنترنت بأنه موضوع مستجد ، ولم يحظ بعد بالاستقرار على النحو الذي حظيت به أنشطة التحقيق في الجرائم التقليدية ، لذا تتحدد مشكلة الدراسة الرئيسة في عدم توفر المعايير القياسية لما يعد صائباً وما لا يعد ، كذلك في ميدان التعامل مع هذه الجرائم وأنشطة مكافحتها ، ويرتبط بالإشكالية الرئيسة أيضاً غياب الخبرة الفنية الملائمة للتحقيق في جرائم تقنية المعلومات وغياب الأدوات التشريعية التي تتيح إمكانية توجيه هذا النشاط ، لهذا فإن غرض الدراسة الرئيسي السعي لتقديم إجابات ملائمة – بتوفيق من الله ومشيئته – للأبعاد الرئيسة والفرعية لهذه الإشكالية.

فروض الدراسة :

تثير هذه الدراسة عدة فرضيات ومنطلقات ، تلخص فيما يلي :

هل يمكن أن تنطلق الدراسة هذه في محاولة للوصول إلى إجابات ملائمة للإشكالية الرئيسة من مجرد فرضية الكفاءة والفعالية في أنشطة مكافحة جرائم تقنية المعلومات ؟؟

وتعتبر هذه الفرضية محدداً هاماً ، بل وهدفاً لأجهزة إنفاذ القانون ، فهي ستؤدي بالضرورة إلى نتائج قد تعارض مشروعية أنشطة التحقيق ، لذا فإن الفرضيات التي تحكم تقديم الحلول للمشكلات المثارة تتمثل فيما يلي : ما يتضمنه التحقيق من إجراءات التفتيش والضبط والتعامل مع الأدلة يخضع للمشروعية القانونية من حيث التقيد بما يقرره القانون لصحة وقانونية وسلامة هذه الإجراءات. كما أن التحقيق في البيئة الرقمية محكوم باحتياجات وقواعد وإجراءات تختلف عن التحقيق في بيئة الجرائم المادية التقليدية ، سواء

من حيث طبيعة السلوك الإجرامي أم من حيث طبيعة الدليل أو وسـائل وآليـات كشـف الجريمة والوصول إلى الدليل الملائم لإثباتها.

وفعالية إجراءات التحقيق في هذا النمط من الجرائم رهن بتـوفر الدرايـة الفنيـة والقانونية معاً لدى جهات مباشرة التحقيق ، وهي دراية متخصصة لا تقتضيها فقط سـلامة إجراءات التحقيق ، بل تتطلبها خطط تفعيل وتطوير أداء الجهة التـي تمارسـها. كمـا أن التحقيق في هذا النمط من الجرائم محكوم بعدم المسـاس بالخصوصـية المعلوماتيـة ، أي حماية البيانات الشخصية المتعلقة بالحياة الخاصة المخزنة في نظم المعلومـات والشـبكات وحماية الأسرار التجارية للمنشآت محل إجراءات التحقيق.

وهذه الفرضيات الرئيسة هي محددات لازمة للحلول والأصول المقترحة ، وتجاوز أي منها يجعل نتائج وتوصيات التعامل مع تحقيق جرائم تقنية المعلومات مهدداً بخطر عدم الملائمة وعدم الفعالية ومخالفة الشرعية. ويقتضي التحقيق في جرائم تقنية المعلومـات أن يكون المحقق خبيراً فاهماً للحاسوب وشبكة المعلومات وعناصرها وأجزائها ، ولذلك يتطلب البحث التعرض لمثل هذه العناصر.

منهج الدراسة :

تعتمد الدراسة على المنهج التحليلي التطبيقي ، حيث تعـرض للجوانـب المتصـلة بالمسألة مدار البحث لتحليلها للوصول إلى الحل أو الموقف منها في ضـوء الاحتياجـات العملية والتطبيقية ، وفي ضوء الأحكام الموضوعية الفنية والقانونية ، وتستند مادة الدراسة من حيث مرجعياتها إلى أحدث الكتب والمؤلفات العربية والأجنبية في هذا الموضوع وإلى مجموعة واسعة من المقالات والأبحاث والتقارير والحالات التطبيقيـة والمنشـورة علـى المواقع المتخصصة على الإنترنت.

معوقات الدراسة :

سبق القول إن جرائم تقنية المعلومات تتسم بأنها ذات طبيعة فنيه ، وأن الدليل على وقوعها سرعان ما يمكن التخلص منه ، ومحوه ، نظرا لارتكاب تلك الجرائم في الخفاء ، فإنه من هذا المنطلق تبدو لنا معوقات دراستها ، وأبرز عائق أمام هذا النوع من الدراسات هو الحاجة إلى تغطيتها من زاويتين: الأولى فنية ، والثانية قانونية. وهو ما يتطلب الإحاطة بجانبي الدراسة توخياً لدقة الحلول والنتائج التي نسعى إلى إظهارها ، بالإضافة إلى مشكلة قلة المراجع العربية المتخصصة. وأن نحاول تذليل هذه المعوقات وتجاوز هذا العائق بما يتوافر من المراجع الأجنبية والدراسات والمقالات المنشورة في مواقع هامة على شبكة الإنترنت.

هيكلة الدراسة وموضوعات البحث :

يتطلب تناول موضوع الدراسة الرئيسي ابتداءً التمهيد لها باستعراض موجز لماهية الحاسوب والإنترنت ، والأجزاء الرئيسية التي تتصل بموضوع الدراسة ، وهو ما نخصص له مبحثا مستقلا ، هو المبحث التمهيدي ، ونظرا لأن موضوع دراستنا هو التحقيق في جرائم تقنية المعلومات ، فإنه يكون من الضروري التعرض بداية للأبعاد المختلفة لهذه الجرائم وإجراءات تحقيقها من حيث سماتها وخصائصها والمخاطر والتهديدات التي تطرحها والمفاهيم الأساسية لها وأهمية دراستها والأهداف التي تسعى الدراسة إلى تحقيقها وذلك كله في فصل تمهيدي ، ثم بيان ماهية التحقيق بصفة عامة ، والقواعد القانونية العامة التي تحكمه وتحديد عام لمشكلات التحقيق في جرائم تقنية المعلومات ، وهذا ما سيكون محلاً للفصل الأول باعتبار هذه الموضوعات مدخلاً موضوعياً يحتاجه الشخص غير المتخصص بالأبعاد الفنية أو القارئ الفني غير المحيط بالأبعاد القانونية.

ولكي يتسنى بحث التحقيق في جرائم تقنية المعلومات لا بد من تحديد منضبط لأنماط جرائم تقنية المعلومات وصورها وذلك على النحو التالي :

المفاهيم الأساسية للدراسة :

1. مفهوم تقنية المعلومات :

يمكن تحديد مفهوم تقنية المعلومات بأنها كل وسيلة الكترونيـــة تســـتخدم لصـــناعه المعلومات أو تخزينها أو معالجتها أو تبادلها أو لعرضها أو تلافيها ومن أمثلتها الحاســـبات الآلية والبرامج والقواعد وبنوك المعلومات ومواقع الويب... الخ.

2. مفهوم جرائم تقنية المعلومات :

ثمة تباين كبير بشأن الاصطلاحات المستخدمة للدلالة علـــى الظـــاهرة الإجراميـــة الناشئة في بيئة الكمبيوتر وفيما بعد بيئة الشبكات ، وهو تباين رافق مسيرة نشـــأة وتطـــور ظاهرة الإجرام المرتبطة أو المتصلة بتقنية المعلومات ، فابتداء من اصطلاح إساءة استخدام الكمبيوتر ، مرورا باصطلاح احتيال الكمبيوتر ، الجريمة المعلوماتية ، فاصطلاحات جرائم الكمبيوتر ، والجريمة المرتبطة بالكمبيوتر جرائم التقنية العالية ، وغيرها ، إلـــى جـــرائم الهاكرز أو الاختراقات فجرائم تقنية المعلومات فجرائم الكمبيوتر والانترنت وأخيرا "السايبر كرايم" ثم جرائم تقنية المعلومات.

واختيار الاصطلاح يتعين إن يزاوج بين البعدين التقني والقانوني ، فإذا عدنا للحقيقة الأولى المتصلة بولادة وتطور تقنية المعلومات ، نجد أن تقنية المعلومات تشـــمل فـــرعين جرى بحكم التطور تقاربهما واندماجهما ، الحوسبة والاتصال ، أما الحوسبة ، فتقوم علـــى استخدام وسائل التقنية لإدارة وتنظيم ومعالجة البيانات في إطار تنفيذ مهام محـــددة تتصـــل بعلمي الحساب والمنطق. أما الاتصال ، فهو قائم على وسائل تقنية لنقل المعلومات بجميـــع دلالاتها الدارجة ، هذه الدلالات هي الرسائل والأخبار والبيانات والمعرفة والوثائق والأدب والفكر والرموز والعلامات والإرشادات الخفية والأنباء المفيدة والسرية وغير ذلك.

ومع تزاوج واندماج وسائل كلا الميدانين (الحوسبة والاتصال) ساد التدليل على هذا الاندماج بالتقنية العالية وهو ما يعرف بتقنيـــة المعلومـــات information technology

والتي تعرفها منظمة اليونسكو بأنها "الفروع العلمية والتقنية الهندسية وأساليب الإدارة الفنية المستخدمة في تداول ومعالجة المعلومات وفي تطبيقاتها ، والمتعلقة بالحواسيب وتفاعلها مع الإنسان والآلات ، وما يرتبط بذلك من أمور اجتماعية واقتصادية وثقافية".

أمام هذا الواقع التقني ، ظهرت مصطلحات عديدة دالة على الأفعال الإجرامية المتصلة بالتقنية ، بعضها دل على الأفعال المتصلة على نحو خاص بالحوسبة ، وبعضها شمل بدلالته قطبي التقنية ، وبعضها دل على عموم التقنية باعتبار ما تحقق من اندماج وتآلف بين مجالاتها ، ومع اتساع استخدام الانترنت ، برزت اصطلاحات جديدة تحاول التقارب مع هذه البيئة المجمعة للوسائط التقنية ولوسائل المعالجة وتبادل المعلومات. أما المنطق لدقة اختيار الاصطلاح ، فيتعين أن ينطلق من أهمية التمييز بين الاصطلاحات المنتمية لما يعرف بأخلاقيات التقنية أو أخلاقيات الكمبيوتر والانترنت ، وبين ما يعرف بإجرام التقنية أو جرائم الكمبيوتر. لهذا مثلاً نجد أن اصطلاح إساءة استخدام الكمبيوتر ينتمي لطائفة الاصطلاحات ذات المحتوى الأخلاقي ، أما جرائم تقنية المعلومات فينتمي لطائفة الاصطلاحات ذات المحتوى الجنائي والقانوني لذلك يجب أن يكون الاصطلاح قادراً على أن يعبر – بقدر الإمكان – عن حدود محله ، فيكون شاملا لما يعبر عنه ، فلا يعبر مثلا عن الجزء ليعني الكل أو يكون على العكس مانع الحدود يطال ما لا ينطوي تحت نطاقه ، ومن هنا ، فان كل اصطلاح وصف الظاهرة بدلالة إحدى جرائم الكمبيوتر كان قاصرا عن الإحاطة الشمولية بالمعبر عنه ، فاصطلاح احتيال الكمبيوتر أو غش الكمبيوتر ونحوه ، مصطلحات أطلقت على أفعال من بين أفعال جرائم الكمبيوتر وصورها وليس الظاهرة برمتها ، وتظل تعبيرات واسعة الدلالة تحيط بأكثر مما تحتوي عليه ظاهرة جرائم تقنية المعلومات وبالنسبة لاصطلاح جرائم المعلوماتية ، والذي وفقا لدلالة الكلمة بوصفها ترجمة عن الفرنسية لمصطلح informatique بمعناها المعالجة الآلية للبيانات استخدم في وصف الظاهرة الإجرامية المستحدثة ، وتبعا لذلك أطلقت تعبيرات جرائم المعلوماتية ، الإجرام المعلوماتي ، التعبير غير دقيق باعتبار المعلوماتية الآن فرعاً مستقلاً من بين فروع المعرفة وعلومها ، ويتصل بقواعد البيانات بوجه عام ، إنشاؤها وإدارتها والحقوق

والالتزامات المتصلة بها. وهو في النطاق القانوني يتعلق بالمعلومات القانونية كان نقـول المعلوماتية القانونية ، ويعالج في نطاقه مسائل توظيف التقنية لإدارة المعلومات القانونية ، وعلى ذات المنوال تقاس بقية طوائف المعلومات المتخصصة.

وهناك تعبيرات شاعت مع بدايات الظاهرة ، واتسع استخدامها حتى عنـد الفقهـاء والدارسين القانونيين ، كالغش المعلوماتي أو غش الحاسوب ، والاحتيـال المعلومـاتي أو احتيال الحاسوب ، ونصب الحاسوب وغيرها مما يجمعهـا التركيـز علـى أن الظـاهرة الإجرامية المستحدثة تتمحور رغم اختلاف أنماط السلوك الإجرامي – حول فعل الغـش أو النصب أو الاحتيال ، لكنه كما أوردنا استخدام لجزء للدلالة على كل فـي حـين أن ثمـة اصطلاحات أكثر دقة للتعبير عن الكل.

ومن بين الاصطلاحات التي شاعت في العديد من الدراسات وتعود الآن إلى واجهة التقارير الإعلامية ، اصطلاح الجرائم الاقتصـادية المرتبطـة بـالكمبيوتر computer-related economic crime ، وهو تعبير يتعلق بالجرائم التي تستهدف معلومات قطاعات الأعمال أو تلك التي تستهدف السرية وسلامة المحتوى وتوفر المعلومات ، وبالتالي يخرج من نطاقها الجرائم التي تستهدف البيانات الشخصية أو الحقوق المعنوية علـى المصـنفات الرقمية وكذلك جرائم المحتوى الضار أو غير المشروع ، ولذلك لا يعبر عن كافة أنمـاط جرائم الكمبيوتر والانترنت.

وهناك أيضا استخدام لاصطلاح يغلب عليه الطابع الإعلامي أكثر من الأكـاديمي ، وهو اصطلاح جرائم ذوي الياقات البيضاء white collar crime ولأن جـرائم الياقـات البيضاء تتسع لتشمل أكثر من جرائم الكمبيوتر والإنترنت ، وتتصل بمختلف أشكال الأفعال الجرمية في بيئة الأعمال بأنواعها وقطاعاتها المختلفة فإن الاصطلاح لذلك لا يكون دقيقـا في التعبير عن الظاهرة مع الإشارة إلى أن جرائم الكمبيوتر تتصف بهذا الوصـف لكنهـا جزء من طوائف متعددة من الجرائم التي يشملها هذا الوصف.

أما عن اصطلاحي جرائم الكمبيـوتر computer crimes والجـرائم المرتبطـة بالكمبيوتر crimes – related computer ، فان التمييز بينهما لم يكن متيسرا في بدايـة الظاهرة ، أما في ظل تطور الظاهرة ومحاولة الفقهاء تحديـد أنمـاط جـرائم الكمبيـوتر والانترنت ، فقد أصبح البعض يستخدم اصطلاح جرائم الكمبيوتر للدلالة على الأفعال التي يكون الكمبيوتر فيها هدفا للجريمة ، كالدخول غير المصرح به وإتلاف البيانات المخزنة في النظم ونحو ذلك ، أما اصطلاح الجرائم المرتبطة بالكمبيوتر فهي تلك الجرائم التي يكـون الكمبيوتر فيها هدفاً أو وسيلة لارتكاب الجريمة ، كالاحتيال بواسطة الكمبيـوتر والتزويـر ونحوهما ، وهناك من يستخدم اصطلاح (السيبر كرايم) كما حدث في النطاق الأوروبـي عموما وانتشر خارجه ، حيث اعتبر هذا الاصطلاح شاملا لجـرائم الكمبيـوتر وجـرائم الشبكات ، باعتبار أن كلمة سايبر تستخدم لدى الأكثرية بمعنى الانترنت ذاتهـا أو العـالم الافتراضي في حين أنها أخذت معنى عالم أو عصر الكمبيوتر بالنسبة للباحثين ولم يعد ثمة تمييز كبير في نطاقها بين الكمبيوتر أو الانترنت لما بينهما من وحدة دمج في بيئة معالجـة وتبادل المعطيات.

التعريف الإجرائي لجرائم تقنية المعلومات

نظراً لاختلاف الاصطلاحات والتعاريف على النحو السابق فإننـا نعتمـد تعريفـاً إجرائياً بأنها كل استخدام غير مشروع لتقنية نظم المعلومات والاتصالات الحديثة مثل شبكة الانترنت والحاسب الآلي والهاتف المحمول أو أحد ملحقاتها أو برامجها بتنفيذ أفعال يجرمها القانون.

3. **مفهوم الدليل التقني:**

هو مكون رقمي لتقديم معلومات في أشكال مختلفة قد تكون نصوصـاً مكتوبـة أو صوراً مرئية أو أصوات مسموعة أو رسومات وأشكال يمكن الحصول عليها من أجهـزة الكمبيوتر وتجميعها وتحليلها باستخدام تكنولوجيا خاصة وطرق علمية بحيث يمكن لأجهزة العدالة الجنائية الاعتماد عليها في تعقب الجريمة التقنية ونسبتها إلى فاعلها.

المبحث الأول
الأبعاد المختلفة لجرائم تقنية المعلومات

المطلب الأول - سمات وخصائص جرائم تقنية المعلومات :

تتسم جرائم تقنية المعلومات بالسمات التالية : [1]

1- من خصائص جرائم تقنية المعلومات أنها ليست جريمة عاديـــة أو تقليديـــة ترتكـــب بصورة عشوائية أو غير مدروسة بل أنها جرائم يحتاج القيام بها إلى خبـــراء علـــي درجة عالية من التخصص والكفاءة في استخدام الحاسب الآلي والانترنت وسعة الأفق والحيلة وأنهم أفراد ذوو مكانة في المجتمع يتمتعون بقدر كاف من العلـــم والتقنيـــة التكنولوجيـــة لما تتطلبه هذه الجرائم من إلمام كاف بمهارات ومعـــارف فنيـــة فـــي مجـــال الكمبيـــوتر والإنترنت وكيفيـــة تشكيله والدخول إليه مما يدعونا إلى القول بأن مرتكبي هذه الجرائم غالبا يكونون من المتخصصين في مجال الانترنت.

2- إن الجرائم مازالت حتى الآن في تحديد الإطار العام محل جدل وتباين في تشريعات معظم دول العالم بل أن معظم الدول لم تسن تشريعات لمواجهة هذه الجرائم.

3- إن هذه الجرائم غالبا ما تتصف بأنها جرائم ناعمة فهي لا تتصف بالعنف او القـــوة عند ارتكابها ولكنها تتم بلمسات بسيطة لا تستغرق سوى ثوان معدودة.

4- في الكثير من الأجيال يكون من الصعب بل من المستحيل ملاحقـــة مرتكـــب هـــذه الجريمة حيث يعمد الكثير من هؤلاء إلى إخفاء أســـمائهم وشخصـــياتهم الحقيقيـــة ويرتكبون جرائم تحت أسماء وهمية أو مستعارة.

5- من الناحية الفنية يصعب توفير رقابة دائمة ومستمرة علـــى الكميـــات والموجـــات المتلاحقة من المعلومات والإعلانات والتي تقـــدر بـــالملايين وتمـــر عبـــر شـــبكة الإنترنت.

1- د. أحمد وهدان ، تقييم فعاليات المواجهة التشريعية لجرائم الانترنت ، الشارقة ، مركز بحوث الشرطة ، مجلة الفكر الشرطي ، مج 13 ، عدد 1 ، إبريل 2004 ، ص 99.

6- إن الجرائم تتسم بأنها جرائم خفية يغيب فيها الدليل المرئي الملموس كما إنها تفتقر إلى الإثارة التقليدية للجرائم العادية على نحو يحول دون الوصول إلى الدليل بيسر وسهولة

7- إن الكثيرين من الضحايا والشهود يحجمون عادة عن الإبلاغ عن جرائم الانترنت حماية للسمعة والشرف والاعتبار خاصة جرائم البغاء وممارسة الجنس والفجور التي ترتكب بواسطة الانترنت

8- إن الباعث الغالب على معظم هذه الجرائم هو النفع المادي السريع ونادراً ما تقع هذه الجرائم بدوافع الانتقام أو التشهير

9- مما يزيد الأثر المضاعف لسلبيات هذه الجرائم أن الدول النامية هي التي تتأثر أكثر بهذه الجرائم فهي الضحية المستهدفة.

10- إن جرائم تقنية المعلومات وخاصة في الدول النامية التي لا تتضمن بنيتها التشريعية نصوصا لتواجه هذه النوعية من الجرائم تعتبر غابة لا يحكمها قانون حيث أن النصوص الجنائية التقليدية وخاصة الإجرائية منها لا يمكنها تغطية كثير من الجرائم التي تقع بواسطة الإنترنت.

11- إن من أبرز خصائص جرائم تقنية المعلومات صعوبة إثباتها وهذا يرجع لعدة أسباب:

أ. أنها جريمة لا تترك أثر ماديا ملموسا.

ب. أنها جريمة يصعب فنيا الاحتفاظ بآثارها

ج. أنها جريمة يصعب على أجهزة إنفاذ القانون التقليدية أن تتفهم حدودها الإجرامية وما تخلفه من آثار مرئية أو ملموسة.

د. أنها جريمة تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.

هـ. أنها جريمة تعتمد على الذكاء المتناهي والحرفية التقنية البالغة في ارتكابها.

12- يمتلك مرتكبو هذه الجرائم القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة.

المطلب الثاني - المخاطر التي تطرحها جرائم تقنية المعلومات :

تطرح الجريمة المعلوماتية أشكالاً عديدة من المخاطر التي تستهدف بصفة مباشـــرة الأمن والاستقرار السياسي والاقتصادي والاجتماعي على المستويين الوطني والدولي.

فمن حيث الخطر على استقرار وسيادة الدول :

يشكل هذا النمط الإجرامي بحكم طبيعته انتهاكاً لحدود وسيادة الدول وتحديا ضـــمنيا أو صريحا لسلطة الدولة في فرض سيادتها على حدودها مما يفقد مفهوم السيادة كثيراً مـــن معناه الحقيقي.

ومن حيث الخطر على المجتمع :

تشكل هذه الجريمة خطراً على النسيج الاجتماعي من حيث التكلفة التـــي يتحملهـــا المجتمع في سبيل تعقب هذه الجرائم وما تحدثه من إخلال بنسق القيم فضلا عـــن شـــيوع الفوضى وانتهاك الحريات والحرمات.

ومن حيث الخطر على الأفراد :

فإن الجريمة المعلوماتية تخلق بيئة غير آمنة بحيث لا يستطيع الأفراد تصريف أمور حياتهم اليومية بدون خوف أو قلق إذ قد يتعرضون لمشاكل المخدرات والاتجـــار بالبشـــر والبغاء والدعارة.

من حيث الخطر على الاستقرار الوطني والديمقراطية :

تتوغل الجريمة المعلوماتية داخل الدولة بشكل مخيف فتصبح دولـــة داخـــل دولـــة تمارس سلوكا ضد الدولة وتهدد استقرارها السياسي والاجتماعي كما هو الحال عند انتشار الجماعات المناهضة وقد يحدث في بعض الحالات إن بعض الحكومات قد تستغل التهديـــد الموجة إليها من الجماعات الإجرامية المنظمة لغرض فرض قيود على الحرية الشخصـــية مما يعني تشويه العناصر الأساسية للديمقراطية.

من حيث الخطر على الاقتصاد والتنمية :

تستهدف هذه الجرائم تحقيق عوائد مالية بالدرجة الأولى بطرق غير مشروعة وغالبا ما يتم إدماج هذه العوائد في الاقتصاد الوطني بقصد تنظيفها وغالبا ما ينعكس هذا البعد انعكاساً سلبياً على الاقتصاد حيث تقوض جهود التنمية والجهود الرامية إلي ضمان التوازن الاقتصادي بالإضافة إلى أن هذه المنظمات تشكل تهديدا خطيرا للبنوك والمؤسسات الاقتصادية والمالية والنظام الإداري الحكومي.

الجانب الإجرائي في جرائم تقنية المعلومات :

يتم التفتيش في هذا النمط من الجرائم عادة على نظم الحاسوب وقواعد البيانات وشبكات المعلومات ، وقد يتجاوز النظام المشتبه فيه إلى أنظمة أخرى مرتبطة به ، وهذا هو الوضع الغالب في ظل شيوع التشبيك بين الحواسيب وانتشار الشبكات الداخلية على مستوى الدول ، وامتداد التفتيش إلى نظم غير النظام محل الاشتباه يخلق تحديات كبيرة أولها: مدى قانونية هذا الإجراء وثانيها: مدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش ، ويتطلب ذلك تحريز جهاز الحاسوب وضبط المكونات المادية في مختلف أجزاء النظام التي تزداد يوماً بعد يوم. والأهم من ذلك أن الضبط ينصب على المعطيات والبيانات والبرامج المخزنة في النظام أو النظم المرتبطة بالنظام محل الاشتباه ، أي على أشياء ذات طبيعة معنوية معرضة بسهولة للتغيير والإتلاف.

وتثير هذه الحقائق مشكلات متعددة ، منها المعايير المقبولة للضبط المعلوماتي ومعايير التحريز إضافة إلى مدى مساس إجراءات ضبط محتويات نظام ما بخصوصية صاحبه ، وفي كثير من الأحيان تتعدى أنشطة الضبط إلى كل محتويات النظام التي تضم عادة معلومات وبيانات قد يحرص على سريتها أو أن تكون محل حماية بحكم القانون أو لطبيعتها أو تعلقها بجهات أخرى.

وتكون أدلة الإدانة ذات نوعية مختلفة ، فهي معنوية الطبيعة كسـجلات الحاسـوب ومعلومات الدخول والبرمجيات [1]. وقد أثارت وتثير أمام القضاء مشكلات جمة من حيث مدى قبولها وحجيتها والمعايير المتطلبة لتكون كذلك خاصة في ظل قواعد الإثبات التقليدية، وبناءً على ذلك ، فإن البعد الإجرائي لجرائم تقنية المعلومات والإنترنت ينطوي على تحديات ومشكلات جمة ، عناوينها الرئيسة ، الحاجة إلى سرعة الكشف عنها خشية ضياع الدليل ، وخصوصية قواعد التفتيش والضبط الملائمة لتلك الجرائم ، وقانونية وحجية أدلة جرائم تقنية المعلومات والإنترنت ، والحاجة إلى تعاون دولي شامل في حقل امتداد إجراءات التحقيق والملاحقة خارج الحدود. وهذه المشكلات كانت وما تزال محل اهتمام على الأصعدة المحلية والإقليمية والدولية.

المبحث الثاني
المشكلات العملية والعلمية في تحقيق جرائم تقنية المعلومات

تمهيد :

نظراً لعدم وجود إطار قانوني إجرائي ينظم إجراءات الضبط والتحقيق في جرائم تقنية المعلومات ، فقد أظهر التطبيق العملي مجموعه من المشكلات والصعوبات تشكل تحدياً أمام مكافحة هذه النوعية من الجرائم يمكن تأصيلها في

المطلب الأول : صعوبات وإشكاليات جرائم تقنية المعلومات :

أولاً – صعوبات التحقيق في جرائم تقنية المعلومات :

1. بالنسبة للدليل المستمد من هذه الجرائم :

1- "هناك ثلاثة نماذج تشريعية لتدابير حماية الخصوصية المعلوماتية وهذه التدابير تعتمد في تطبيقاتها على ما إذا كان منطلق النظام القانوني مجرد الاعتراف بالخصوصية معتمدا على إباحة كل ما يدخل في نطاق الحق أهمية باستخدام وسيلة مواجهة الأنشطة التي تمثل اعتداء على الخصوصية" للمزيد الجنبيهي منير محمد : أمن المعلومات الالكترونية ، الإسكندرية : دار الفكر الجامعي ، 2006 ، ص77.

أ. صعوبات تتعلق بالدليل الالكتروني من حيث نمطه وتحليله.

ب. صعوبات تتعلق بالحجية القانونية للدليل الالكتروني.

ج. صعوبات تتعلق بتقنين الدليل في جرائم تقنية المعلومات.

2. بالنسبة لعملية إجراء التحقيق في جرائم تقنية المعلومات.

أ. صعوبات تتعلق بقلة العناصر المدربة(شرطة-نيابة-قضاء).

ب. صعوبات تتعلق بالمعامل اللازمة للتحليل والتحقيق.

3. بالنسبة لصيغة جرائم تقنية المعلومات.

أ. صعوبات تتعلق بحداثة موضوعات هذه الجرائم وتطورها السريع.

ب. صعوبات تتعلق بالتكنولوجيا المطروحة لارتكاب هذه الجرائم.

ج. صعوبات تتعلق بالطبيعة الدولية لهذه الجرائم.

4. بالنسبة للإطار القانوني لضبط وتحقيق هذه النوعية من الجرائم.

أ. غياب الإطار القانوني الإجرائي الخاص.

ب. غياب أجهزة شرطة ونيابة وقضاء متخصصة للتحقيق والحكم في هذه الجرائم (1).

يلاحظ من استعراض أهم المحاور المتعلقة لعملية الضبط والتحقيق والصعوبات التي تواجه ضبط الجرائم لتقنية المعلومات أن البحث عن مرتكبي الجرائم المعلوماتية وإقامة أدلة الإثبات عليهم وتقديمهم للعدالة للقصاص منهم يواجه العديد من الصعوبات خاصة في مجال الإثبات الجنائي والشرعية الإجرائية الواجب الاستناد إلى قواعدها حتى يتصف الدليل الجنائي بالمشروعية ويجب أن تكون وسيلة الحصول على الدليل مشروعة حتى يوصف الدليل بأنه دليل شرعي ، وقد يكون الدليل شرعياً ، إلا إن وسيلة الحصول عليه هي التي توصف بعدم المشروعية مما يجعل البطلان ينصرف إلى قيمة الدليل في الإثبات ولعل من أهم الصعوبات التي تواجه ضبط جرائم الإرهاب الاليكتروني ما يلي :

1- د. محمد السعيد ، الإرهاب الالكتروني ، القاهرة : مجلة الأمن العام ، العدد 206 ، السنة 51 ، يونيو 2009 ، ص97.

- سهولة إخفاء الجريمة.
- صعوبة الوصول إلى مرتكبي الجريمة. حيث يعتمد الإرهــاب الإلكترونـــي علــى التكنولوجيا المتطورة والتي زادت من واقعة مسرح العمليات واتساعه بطريقـــــة فائقة.
- نقص الخبرة لدى القائمين على ضبط الجرائم المعلوماتية وإقامة الدليل.
- صعوبة الإثبات ، ومرد ذلك إلى الطبيعة الخاصة للدليل في الجــرائم المعلوماتيــة لكونه دليلاً غير تقليدي ، بالإضافة لصعوبة الوصول لهذا الدليل ، وســهولة محــو آثاره.
- تعارض التفتيش عن الأدلة في الجرائم المعلوماتية مع الحق في الخصوصية ، نظراً لكون التفتيش عن الأدلة في الجرائم المعلوماتية لا يكون في محل محدد كــالجرائم التقليدية التي يحدد فيها على وجه الدقة المكان الذي سيجرى فيه التفتــيش والــدليل الجاري البحث عنه. حيث إن التفتيش هنا ينصب غالباً على نظم الحاسب الآلــي ، وعلى قواعد البيانات ، ونظم المعلومات وشبكاتها ، مما يؤدي حتماً إلــى تجــاوز المشتبه فيه محل التفتيش إلى أنظمة أخرى مرتبطة به سواء في الشبكات الدولية أو الشبكات المحلية بالإضافة إلى أن التفتيش عن الأدلة الرقمية يحتاج إلى توافر خبرة فنية عالية لدى القائمين بالتفتيش.
- إحجام بعض الأشخاص والهيئات والمؤسسات عن الإبلاغ عن الجرائم المعلوماتيــة خشية التشهير أو الإساءة للسمعة المالية للجهة وخوفاً من فقدان الثقة في التعامل.
- التعارض القائم بين تجاوز الحدود لضبط الجرائم المعلوماتية والمبــادئ القانونيــة المعمول بها في الدول والتي تحكم تطبيق القانون من حيث المكان مما يجعل الحاجة ملحة لنصوص تشريعية تنظيم هذا الأمر وتحتاج إلى نوع مــن التعــاون الــدولي لمكافحة تلك الجريمة مع الحفاظ على ثوابت السيادة الوطنية للــدول لكــون تلــك الجريمة من الجرائم العابرة للحدود.

ثانياً – مشكلات التحقيق في جرائم تقنية المعلومات :

وهذه الصعوبات من شأنها أن تثير العديد من المشكلات العملية المتعلقة بالإجراءات الجنائية عند ضبط جرائم تقنية المعلومات مثل : [1]

1- إن قيام النيابة العامة بإصدار أمر التفتيش في إحدى هذه الجرائم يقتضي إن يكون مصدر الإذن على دراية وخبرة فنية جيدة بالكمبيوتر وشبكة الانترنت واستخدامها والوصول إليها بحيث يكون إذن الضبط والتفتيش محددا وموصوفاً بطريقة علمية وفنية منتجاً لآثاره عند طرح الدليل المنبثق عنه أمام القضاء.

2- سهولة تدمير المعلومات المؤدية إلى معرفة شخصية المجرم بمجرد علمه بصدور إذن بضبطه أو تفتيشه نظراً لأن جرائم تقنية المعلومات غالباً ما ترتكب من أشخاص على درجة عالية جداً من الخبرة والدراية بتقنيات الكمبيوتر والانترنت ، وبالتالي يصعب تقديم دليل قوي تقتنع به المحكمة لإدانة المتهم وعقابه.

3- ممن يصدر الإذن بالضبط والتفتيش في جرائم الكمبيوتر ؟ هل من النيابة العامة باعتبارها سلطة تحقيق لها الحق في الإذن بضبط الأجهزة محل الجريمة ، ام يجب إصدار هذا الإذن من القاضي الجزائي باعتبار إن الإذن بالتفتيش في مجال جرائم تقنية المعلومات إنما هو إذن بمراقبة معلومات وأفعال تبث عبر خط تليفون بدونه لا يمكن الاتصال بشبكة المعلومات الدولية (الانترنت) وذلك طبقا لنص المادة (95) من قانون الإجراءات الجنائية.

4- لم تنل الجرائم المرتكبة عبر شبكة الانترنت اهتماماً كبيراً في مصر وخاصة فيما يتعلق بالمواجهة الجنائية ، وربما يرجع السبب الرئيسي إلى كون هذه الجرائم مستحدثه ولم تنتشر في مصر إلا مع انتشار استخدام شبكة المعلومات الدولية أي منذ سنوات معدودة ، وهكذا يصبح كثير من الأمور الأخلاقية والشخصية والمعلوماتية والمالية غير محمية بنصوص القانون الجنائي وخاصة ما يتعلق منا بالجانب الإجرائي ولذا تجد سلطات إنفاذ القانون صعوبات كبيرة عن ضبط

1- د. أحمد وهدان ، تقييم فعاليات المواجهة التشريعية لجرائم تقنية المعلومات ، مرجع سابق ، ص110.

وتحقيق كثير من هذه الجرائم والأمر متروك للفقه والقضاء من أجل بسط النصوص التقليدية القائمة على هذه الوقائع ، من حيث أنه من الأيسر والأصوب أن يلتفت المشرع إلى هذه المشكلة ويفرد لها تشريعاً خاصاً ينص على تجريم صور العدوان والأفعال غير المشروعة المتصور حصولها عبر شبكة الانترنت.

5- ومن ناحية جمع عناصر الإثبات ، فقد اعتادت سلطات الضبط والتحقيق جمع عناصر الإثبات الجنائي بطرق تقليدية عن طريق الضبط والتفتيش المادي الملموس ، بيد إن هذه الإجراءات التقليدية يصعب القيام بها في حالات جرائم تقنية المعلومات.

6- كذلك تتضح صعوبة إثبات هذه الجرائم في أنها غالباً تترك أثرا خارجياً ملموساً كعدم وجود أثر كتابي كما إن الجاني يستطيع تدمير دليل الإدانة بسرعة بالإضافة إلى أن ارتكاب هذه الجرائم يتم عادة من مسافات بعيدة وباستخدام الخط التلفوني الذي يمكن الجاني من إعطاء تعليماته بتنفيذ مشروعه الإجرامي من على بعد.

7- وحتى بفرض تمكن أجهزة الضبط والتحقيق من جمع أدلة من خلال الانترنت تثبت ارتكاب الفعل ونسبته للمجرم فإن المشكلة لا تزال قائمة في مدى مشروعية هذه الأدلة في الإثبات واقتناع القضاء بها.

ثالثاً – إشكاليات إثبات جرائم تقنية المعلومات :

القصور التشريعي وندرة التطبيقات القضائية :

يبرز للوجود صعوبة جمع الاستدلالات والأدلة في الجريمة المعلوماتية حتى يمكن تحقيق عناصرها والتصرف فيها لكونها تعتمد على مجرد نبضات الكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الكمبيوتر والبيانات التي يمكن استخدامها كأداة ضد الفاعل يمكن العبث بها أو محوها بالكامل في لحظة زمنية (فمتوثانية) ، ولهذا يمكن القول إن المصادفة لها دور كبير في اكتشافها أكثر مما هو متوقع من أساليب الرقابة والتفتيش والمراجعة على الحاسبات الآلية ، ويختلف إثبات الجريمة المعلوماتية عن كافة الجرائم الأخرى سواء من

حيث وسيلة الإثبات أو القائم بها ومدى الخبرة المعلوماتية التي تتوافر لديه وهي بلا شك إحدى الثغرات التي يعتمد عليها ذكاء المجرم المعلوماتي الذي غالباً ما يتمتع بدرجات عالية من المهارة في فنون التعامل مع الحواسب الآلية ، ولهذا فهناك بلا جدال مشاكل عديدة في كيفية إثبات تلك الجرائم [1].

والجريمة المعلوماتية كغيرها من الجرائم تقوم على ذات الأركان والعناصر وتمر الدعوى الجنائية فيها بنفس المراحل الخاصة بسائر الجرائم ، كما أن ارتكابها يقتضي التفكير في الجريمة والتحضير لها (الشروع) ،ثم تنفذيها ومحاولة التخلص من آثارها ، ولذلك تثور هنا مسألة استخلاص الدليل الذي تثبت به الجريمة المعلوماتية ، وإذا كان الاعتراف وشهادة الشهود والقرائن والآثار الناجمة عن النشاط الإجرامي لها دور في إثبات هذا النوع من الجرائم المعلوماتية وكشف الحقائق فيها وهي أمور تعين المحقق على استجواب المتهمين وسؤال الشهود ، إلا أن ذلك يبدو قاصراً في ملاحقة مرتكبي الجريمة المعلوماتية.

لذا فقد كان لظهور تلك النوعية من الجرائم دور أساسي في قيام كثير من الدول بسن تشريعات جديدة أو تعديل تشريعاتها القائمة لمواجهة فنون الجريمة الحديثة ومشكلاتها القانونية والتي تتعلق بكيفية حماية المعلومات والبرامج ذات الصلة ، إن ذلك لا يعني بالضرورة أن يكون المحقق خبيراً في علوم الحاسب الآلي – وإن كان هذا أفضل – ولكن يجب أن يلم ببعض المسائل الأولية التي تمكنه من التفاهم مع خبراء منظومة المعلومات وحسن استغلالهم في كشف الجرائم وجمع الأدلة ، كما أنه من الضروري أن يكون المحقق ملماً بالإجراءات الاحتياطية التي ينبغي اتخاذها نحو مسرح الجريمة المعلوماتية والتدابير اللازمة لتأمين الأدلة.

1- اشرف صلاح الشيخ ، الجريمة المعلوماتية ، مجلة الأمن العام : القاهرة ، العدد 206 ، السنة51 ، يونيو 2009 ، ص117.

ومن هنا تبدو الأهمية لكيفية إجراء الاستدلالات واســتخلاص الــدليل فــي مجــال الإجرام المعلوماتي ، وقد تكون صعوبة استخلاص الدليل تعود إلى الدليل ذاته من حيث إنه دليل خفي غير مرئي ، إلى جانب أن معظم الجرائم المعلوماتية لا تترك أثراً ملموساً ، كما أنها تستعصي على أساليب البحث التقليدية ، وتظهر أيضاً مشكلات في استخلاص الــدليل لصعوبات تتعلق بحجم وكم البيانات ، وسهولة تدميرها من الجناة.

التفتيش في مجال المعالجة الإلكترونية للمعلومات :

التفتيش كأحد إجراءات التحقيق في الجريمة يثير مشكلات عملية في مجال المعالجة الآلية للمعلومات ، حيث إن الجريمة المعلوماتية المطلوب إثباتها وإن كانت محددة بوقــت معين ووقائع محددة يسهل تعيينها ، إلا أن الأمر ليس كذلك دائماً ، فقد تتعقد مهمة المحقق لأنه سوف يصادر على أو يطلع على كافة محتويات الحاسب الآلي ، مما قد يشكل اعتــداءً أو إساءة لاستخدامها السلطة حينما يمتد نشاط المحقق بعيداً عن الواقعة الإجرامية ، وبالتالي يتجاوز ويمس الحق في خصوصية الأفراد ، حينما يكــون نشــاطه بعيــداً عــن الواقعــة الإجرامية المعلوماتية التي يجري بشأنها التحقيق ، والذي يحق للشخص المحافظــة علــى سريته ، ذلك أن كشف الأسرار في هذه الحالة قد يدفع الفــرد (أو المشــروع " مصــنع أو شركة... الخ) إلى تعطيل أو وقف التحقيق الذي تكون محله المعلومات المعالجة الكترونيا.

المطلب الثاني - الأصول الفنية الواجب مراعاتها للتحقيق في الجريمة المعلوماتية:

1- تدريب القائمين من سلطات (جمع الاستدلالات والتحقيق والمحاكمة) على الحاسبات الآلية:

ولذلك يجب تدريب وتأهيل القائمين على جمع الاســتدلالات والتحقيــق الابتــدائي والحكم في جرائم الحاسبات الآلية ، سواء فيما يتعلق بالأساليب الفنيــة المســتخدمة فــي ارتكاب الجريمة ، أو فيما يتعلق بطرق الكشف عنها ، والقرائن والدلائل والأدلة المستخدمة في مجال إثباتها وكيفية معاينتها والتحفظ عليها ، وكيفيه فحصها فنيا ، وتدريب القضاة على

معالجة هذا النوع من القضايا التي تحتاج إلى خبرات عالية ، وذلك حتى يمكنهم قبول الأدلة الناشئة عنها في الإثبات وتقديرها ، وحتى يتمكنوا في النهاية من الفصل في القضايا المتعلقة بهذا النوع من الجرائم ، كما ينظم البوليس الدولي دورات تدريبية في مجال شبكات الحاسبات الآلية من أجل تحسين أداء الأعضاء من رجال الشرطة في مجال الكشف عن الجريمة وجمع المعلومات ومتابعة الجناة وإقامة الدليل في الجرائم التي ترتكب في هذا المجال ، ونرى ألا يقتصر التدريب على رجال الشرطة فقط بل يجب أن يمتد ليشمل رجال القضاء.

2- التدريب على كيفية جمع الأدلة وإجراء التحقيق :

يفرض تحقيق جرائم الحاسب الآلي منهجاً معيناً على مأموري الضبط القضائي والمحققين في سبيل البحث عن مرتكبي هذه الجرائم وإقامة الدليل على المساهمين فيها ، ولذا يوصي الخبراء بالاسترشاد ببعض الإجراءات في مرحلتي التحريات والتحقيق الابتدائي:

أ – في مرحلة التحريات.

يجب اتباع بعض الإجراءات الهامة مثل :

- تحديد نوع نظام المعالجة الآلية للمعلومات.
- وضع خطة إجمالية للمنشأة وإعداد كشف بأسماء المسئولين عنها ودور كل منهم.
- الدليل يمكن أن يختفي في أي وقت.
- في استطاعة الجاني التدخل لإتلاف المعلومات.
- فصل التيار الكهربائي من مكان خارج الموقع قبل دخوله وكذا خطوط التليفون.
- التأكد من عدم استخدام خاصية تحويل المكالمات الهاتفية.
- إبعاد جميع الموظفين عن أجهزة الحاسبات الآلية.

ب – في مرحلة التحقيق الابتدائي.

يجب أيضا اتباع بعض الإجراءات الهامة مثل :

- عمل نسخة احتياطية من الأقراص الصلبة أو الاسطوانات المرنة قبل اســتخدامها في البحث والتحقيق.
- نزع غطاء الجهاز المستهدف.
- تحديد الملفات الممسوحة الممكن استعادتها من سلة المهملات.
- إجراء بحث نصي على الكلمات الهامة المتعلقة بالقضية.

المبحث الثالث
إجراءات التحقيق في جرائم تقنية المعلومات

تمهيد و تقسيم :

يقتضي البحث في إجراءات التحقيق في جرائم تقنية المعلومات التعرض لأهــم هــذه الإجراءات بشيء من التفصيل حيث نخصص المبحث الأول لدراسة الانتقال (انتقال المحقــق) والمبحث الثاني نبين فيه المعاينة في جرائم تقنية المعلومات أما المبحــث الثالــث فنخصصــه للتفتيش في الحاسوب والانترنت والتقنية المعلوماتية في حين نتناول في المبحث الرابع الاستعانة بالخبراء لكشف غموض هذه الجرائم في حين نخصص المبحث الخامس لشهادة الشهود ودورها في إثبات هذه الجرائم ونختتم هذا الفصل بتناول أحكام الضبط في مجال جرائم تقنية المعلومات في المبحث السادس.

المطلب الأول - الانتقال (انتقال المحقق):
المقصود بالانتقال والهدف منه :

طبقا لما ورد بقانون الإجراءات الجزائية الإماراتي ينتقل المحقق إلى أي مكان كلما رأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ، ووجود الجريمة ماديا ، وكل ما يلــزم إثبات حالته ، ويقصد بالانتقال " ذهاب المحقق إلى محل الحادث أو إلـــى مكـــان آخــر ، ارتكبت فيه الجريمة أو تحققت فيه آثارها وماديتها ، لمعاينته" ، وإذا وجدت جرائم لا يلزم فيها مباشرة هذا الإجراء ، كجرائم الرشوة مثلا ، فإن جرائم تقنية المعلومـــات تقتضـــى ــ بحسب طبيعتها ــ إجراء الانتقال إلى مكان وقوع الجريمة ومعاينة الأدلة على وقوعهـــا ،

علاوة على معاينة المضبوطات التي تجلب للمحقق في مقر عمله ، كالمستندات المزورة ، من جوازات سفر ، وبطاقات ائتمانية... الخ [1].

المطلب الثاني - المعاينة:

المقصود بالمعاينة وأهميتها في جرائم تقنية المعلومات :

يقصد بالمعاينة " إثبات حالة الأشخاص والأمكنة والأشياء ذات الصلة بالجريمة قبل أن تنالها يد العبث والتخريب " [2]. أو هي " إجراء من إجراءات التحقيق ينتقل بمقتضاه المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه حالة شيء أو شخص معين ، ويجمع الآثار المتعلقة بالجريمة وكيفية ارتكابها ، وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة " [3].

أهمية المعاينة في جرائم تقنية المعلومات :

" تظهر أهمية المعاينة في مجال إثبات الواقعة ونسبتها إلى مرتكبها بما تتضمنه من الحفاظ على مسرح الجريمة باعتباره مستودع سرها ومفتاح كشف غموضها" فهي:

أ- تعبر تعبيرا صادقا ، وبصورة صحيحة وواقعية عن مكان الجريمة ، وما فيه من ماديات وآثار للجاني ، وتكشف عن كيفية تنفيذها من بدايتها حتى نهايتها.

ب- تفيد في جمع الأدلة التي تخلفت عن الجريمة ، وحصر ما بجسم الجريمة من آثار.

1- تماثل المادة (90) من قانون الإجراءات الجنائية المصري ، الدكتور حسني الجندي : قانون الإجراءات الجزائية في دولة الإمارات العربية المتحدة معلقا عليه ، مرجع سابق ص 612.

2- الدكتور محمد عيد الغريب : الاختصاص القضائي لمأمور الضبط القضائي في الأحوال العادية والاستثنائية ، سنة 2003 ص 42.

3- الدكتور حسني الجندي : في شرح قانون الإجراءات الجنائية ، مرجع سابق ص639 ــ وفي ذات المعنى: لنفس المؤلف : قانون الإجراءات الجزائية في دولة الإمارات العربية المتحدة معلقا عليه ، مرجع سابق ص 612 ــ وفي هذا المعنى أيضا : عبد الواحد موسى : التحقيق الجنائي علم وفن بين النظرية والتطبيق ، سنة 1993 2ص 5 دار الكتاب ــ عادل عبد الله خميس : التفتيش كإجراء من إجراءات التحقيق الابتدائي في القانون المصري والإماراتي ، دراسة مقارنة ، رسالة ماجستير ، القاهرة سنة 1998 ص 15.

ج- إعطاء المحقق الفرصة ليلمس بنفسه ــ وعلى الطبيعة ــ العناصر المادية التي تفيد في كشف الحقيقة.

د- بالنسبة للجاني ، نجد أن المعاينة يمكن أن تكشف عن ملامح شخصية الجاني ومهاراته من خلال أسلوبه الإجرامي الذي ارتكب به الجريمة ، والتعرف على الغرض من ارتكابها ، والباعث عليها ، وعدد الجناة وعلاقتهم بالمجني عليه [1].

وبتطبيق ذلك على جرائم تقنية المعلومات والانترنت ، نجد أن نزع أو نقص في أجزاء الحاسوب إذا كانت الجريمة هي سرقة وقت على محتويات الحاسوب وأدواته. علاوة على أنه بمناظرة هذا الحاسوب ، وبالولوج إلى شبكة الانترنت نستطيع التعرف على بصمة الجاني ، وغيرها من الآثار التي تفيد بحدوث اختراق للمواقع التي تتعلق بالمجني عليه.

ويقال أن للمعاينة دوراً أقل من دورها بالنسبة للجرائم التقليدية. ويرجع ذلك إلى قلة الآثار المادية ، وكثرة المترددين على مسرح الجريمة ، وسرعة تغيير أو محو تلك الآثار ، نظرا لطبيعتها الخاصة [2]. ولذلك ينبغي مراعاة بعض الأمور الفنية ، كتصوير الحاسوب والأجهزة المتصلة بها ، وملاحظة طبيعة النظام المستخدم ، والحرص الشديد عند نقل المواد المعلوماتية.

شروط إجراء المعاينة :

تتطلب صحة إجراء المعاينة المعلوماتية توافر الشروط الآتية:

1- أن تكون الجريمة مما تقبل المعاينة بطبيعتها. وهنا يمكن القول بأن الجرائم المعلوماتية تقبل المعاينة ، فلا يتطلب ذلك سوى ملاحظة الحاسوب والدخول إليه ، والنظر إلى أجزائه وأدواته ، ليتبين المحقق ما هي الأجزاء التي سلبت منه ، ومحاولة استرجاع

1- العقيد سامي حارب المنذري : موسوعة العلوم الجنائية ، تقنية الحصول على الآثار والأدلة المادية ، المجلد الأول ، مركز بحوث الشرطة ، الشارقة ، الإمارات ط 1 سنة 2007 ص 683.

2- محمد علي عبيد المحواث الحمودي : دور مأمور الضبط القضائي في مواجهة جرائم المعلومات ، مرجع سابق ص 157.

البرامج والبيانات التي تمت كتابتها ، ثم طمست أو دمرت ، وما طرأ على الجهاز من فيروسات تم نشرها عليه.

2- أن يتم الانتقال بسرعة ، حتى لا يتطرق الشك إلى الدليل المتحصل من الحاسوب أو شبكة الانترنت. فإذا انقضت فترة زمنية طويلة بين وقوع الجريمة وبين إجراء المعاينة، بحيث تسمح للجاني بإزالة بعض الآثار أو العبث بالدليل ، فإن المعاينة تكون غير مجدية.
3- أن يكون الانتقال والمعاينة لازمين لكشف حقيقة الجريمة ونسبتها إلى متهم معين.
4- ويمكن أن تجرى المعاينة في حضور المتهم ، كما يمكن أن يقوم بها المحقق في غيبة المتهم [(1)].

صور المعاينة :

للمعاينة صور متعددة ، يقوم بها المحقق بحسب طبيعة الجريمة ، وعلى الخصوص بالنسبة للجريمة التقليدية. أما بالنسبة للجريمة المعلوماتية ، فإنه قد تتناسب معها صور من المعاينة ، منها على سبيل المثال : المعاينة المكانية ، والمعاينة العينية أو المادية ، كالمعاينة التي تتعلق بالأشياء ، والأدوات والآلات الموجودة بمكان الواقعة ، وبيان ما إذا كان بها آثار تفيد في كشف الحقيقة ، كبصمات أو غيرها ، وقد يقوم مأمور الضبط القضائي بالمعاينة بنفسه لتسهيل تحقيق الوقائع التي تبلغ إليه ، واتخاذ الإجراءات التحفظية للمحافظة على أدلة الجريمة ، ووضع الأختام على الأماكن التي أجرى فيها المعاينة. وقد يقوم بها عضو النيابة العامة بنفسه بالمعاينة بمجرد إخطاره بجريمة متلبس بارتكابها. وفي غير ذلك يكون الأمر متروكا لتقدير السلطة التي تباشر التحقيق.

ونظرا لحداثة الجرائم المعلوماتية ، والقضاء على الصعوبات التي تواجه السلطات المختصة ، فإنه ينبغي اتباع مجموعة من القواعد والإرشادات الفنية عند إجراء المعاينة :

1- نقض جنائي مصري جلسة 1980/1/31 مج الأحكام س 31 رقم 29 ص 149.

- تصوير النظام المعلوماتي وما يتصل به من أجهزة طرفية ، ومحتوياته ، وأوضاعه المكانية ، والعناية بصفة خاصة بتصوير أجزائه الطرفية ومخلفاته الأخرى [1].
- إثبات حالة التوصيلات والكابلات المتصلة بمكونات النظام للقيام بالمقارنة والتحليل عند عرض الموضوع على المحكمة.
- عدم التسرع في نقل أي مادة معلوماتية قبل إجراء الاختبارات اللازمة للتـيقن مـن عدم وجود مجالات مغناطيسية تلغي البيانات المخزنة. وحفـظ الأوراق والملفـات الممزقة والأقراص غير السليمة ومخرجات الأجهزة المعلوماتية.

المطلب الثالث - التفتيش:

المقصود بالتفتيش ودوره في جرائم تقنية المعلومات :

التفتيش إجراء من إجراءات التحقيق تقوم به سلطة حـددها القـانون ، ويسـتهدف البحث عن الأدلة المادية لجريمة تحقق وقوعها في مكان معين أو في محل خاص ، أو في مستودع السر الذي يتمتع بالحرمة بغض النظر عن إرادة صاحبه [2].

ولا يختلف التفتيش في جرائم المعلومات عن التفتيش في الجرائم التقليدية ، سـوى في أن الإجراء الأول يهدف إلى الدخول إلى نظم المعالجة الآلية للبيانات بما تشـمله مـن مدخلات وتخزين ومخرجات ، لأجل البحث فيها عن أفعال غير مشروعة مرتكبة وتشـكل جناية أو جنحة ، والتوصل إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابهـا ، ويعتبر التفتيش في مجال الجرائم المعلوماتية من أخطر الإجراءات الجزائية التي تباشر ضد

1- محمد علي عبيد المحواث الحمودي : دور مأمور الضبط القضائي في مواجهة جرائم المعلومات ، مرجع سابق ص 159.

2- الدكتور حسني الجندي : قانون الإجراءات الجزائية في دولة الإمارات... مرجع سـابق ص 494 ومـا بعدها.

مرتكب جريمة ناشئة عن استخدام الحاسوب أو شبكة المعلومات ، نظـرا لطبيعـة الـدليل وصعوبة الوصول إليه [1].

1- السبب :

يجري التحقيق بخصوص جريمة تحقق وقوعها بالفعل ، كجريمة اختراق الحاسوب، والحصـول على المعلومات المخزنة فيه بدون تصريح (م2 من القـانون رقـم 2 لسـنة 2006) ، وجريمة تزوير مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية المعترف بها قانوناً في نظام معلوماتي (م3 من ذات القـانون)... إلخ ، وتثير هذه الجرائم تحديات كبيـرة بشـأن الإطـار القـانوني الملائـم لإجـراءات التحقيق(كالتفتيش والضبط) التي تباشرها سلطات التحقيق المكلفة بتقصي الجـرائم وإحالـة الجناة إلى القضاء ، وتطبيقا لذلك لا يجـوز أن يكون التفتيش من أجـل ضـبط جريمـة مستقبلية ، ولو دلت التحريات على أنها سوف تقع حتماً ، فمتى كانت الجريمة قـد وقعـت فعلاً فلا يشترط فيها أن تكون من نوع معين وتستحق قدرا معينا من العقوبة [2].

2- محل التفتيش :

يقصد بمحل التفتيش المستودع الذي يحتفظ الشخص فيه بالأشياء المادية التي تحتوي على أسراره التي تتعلق بالجريمة المنسوبة إليه ، ويكون محل التفتيش في مجـال جـرائم تقنية المعلومات ، هو الحاسوب والإنترنت من ناحية ، والمعلومـات والبيانـات المخزنـة وأدواته من ناحية أخرى ، ويثور هنا البحث في مدى توافر شروط محل التفتيش في جرائم تقنية المعلومات والانترنت؟ ، وإذا كان يشترط في محل التفتيش أن يكون معينا ، فقد يلاقي المحقق صعوبة في كيفية تعيين الدليل الذي يبحث عنه في آليات الجريمة المنسـوبة إلـى المتهم.

1- الدكتور هشام فريد رستم : الجوانب الإجرائية... مرجع سابق ص 62 وما بعدها.

2- ولكن ذلك لا يمنع من وجوب العمل على منع وقوعها ، وهو ما يندرج ضمن مهام واختصاصات الضبط الإداري.

ويأخذ محل التفتيش في جرائم تقنية المعلومات والانترنت الحاسوب ذاته كأداة في ارتكاب الجريمة. فالجريمة في هذه الصورة لا تقع على الحاسوب ذاته ، ولكنها تقع باستخدامه كوسيلة لتنفيذ هذه الجريمة. مثال ذلك : استخدام الحاسوب في ارتكاب جريمة تزوير المستندات المعترف بها قانوناً في نظام معلوماتي (م4 من القانون رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات الاتحادي) ، وجرائم تزييف العملة المتداولة قانوناً (م204 من ذات القانون).

وتثير جرائم تقنية المعلومات والإنترنت تحديات كبيرة بشأن الإطار القانوني الملائم لإجراءات التفتيش والضبط التي تباشره سلطات التحقيق المكلفة بتقصي الجرائم وإحالة الجناة للقضاء ، ويبدو أن هذا الإطار يغاير أطر التفتيش والضبط المتصلة بالجرائم التقليدية ، ويرجع ذلك إلى أن تقنية الحاسوب تنطوي على حالات مختلفة من حيث ظروفها وأحوالها ، وتتطلب لإجراء التفتيش تقنيات معينة تتناسب وتفتيش نظم المعلومات. فقد لا يكون النظام محل التفتيش للمشتبه به ، وليس ثمة وسيلة ميسرة لمعرفة ذلك.

كما أن ملفات الحاسوب قد تكون مخبأة أو محمية داخل نظام الشخص ، وقد تنتقل حول العالم من نظام لآخر في وقت وجيز. علاوة على أنه يسهل إتلافها بمجرد استخدام لوحة المفاتيح ، ربما ليس إتلافاً كاملاً ، ولكنه قد يكون معطلاً لإنجاز التفتيش عندما لا يكون من يجري التفتيش خبيراً في تقنيات التحري عن الملفات المحمية أو المتلفة ، كما أن الدليل نفسه يصعب تحديد مكانه ابتداء ، فقد يكون داخل النظام أو يكون مخزناً على وسائط أخرى ، كتخزينه على الأقراص باختلاف أنواعها ، وقد يكون موجوداً أصلاً في جزء من الشبكة لا يرتبط بالمشتبه به مباشرة ، لكنه يستخدم هذا الموقع لإخفاء الأدلة أو لتمثل مدخلاً إلى نظم الحاسوب المستهدفة.

والملفات أيضاً قد تكون مشفرة لا يظهر محتواها إلا بفك التشفير ، وقد تكون البيانات التي تثبت حصول الفعل جزءاً من خادم نظام حاسوب يقع خارج الحدود في دولة

أخرى ، وقد يكون نشاط الجاني مباشراً بالأساس من حاسوب لا يخصه أو من حاسوب محمول يسهل عليه التخلص منه أو إنكار ملكيته له ، كل هذه الحقائق وغيرها تجعل من الصعب تحديد السبب الموجب للتفتيش ، وتجعل من تقديم وصف محدد لمحل التفتيش أمراً أكثر صعوبة.

3- أثر التفتيش :

يعتبر الضبط هو الأثر المباشر للتفتيش. وهو بذاته يكون من إجراءات التحقيق التي تهدف إلى وضع اليد على الأدلة المتحصلة من التفتيش وتحريزها وحفظها لمصلحة التحقيق وضبط الأدلة الكونية أو ما يتعلق بجرائم تقنية المعلومات والإنترنت ، وما يتصل بضبط المكونات المادية لأنظمة الحاسوب ، وضبط المكونات المعنوية – البرمجيات ، والمعطيات التي تتناقل أو يجري تبادلها في نطاق شبكة المعلومات التي تربط الحواسيب معاً وما يتصل بها.

وبالنظر إلى أن مكونات نظام الحاسوب المادية من الأشياء ، فإنها في الأصل أشياء مادية يجوز ضبطها وتحريزها. أما بالنسبة للشبكات فإن ما يعني التحقيق في الغالب ، هو المعطيات المستخرجة من الخوادم والأجهزة التي تحكم وتسيطر على هذه الشبكات ، فإن تحصلت عليها جهة التحقيق من الجهة المعنية وفق ما يقرره القانون وما يجيزه – إن لم تكن هي المستهدفة بالتفتيش والضبط – ليس ثمة مشكلة ، أما إن لم يتم تحصيلها وتوفر الموجب لضبط خادم الشبكة – النظام المتحكم بالشبكة – وأجاز القانون والقضاء ذلك ، فإن ما يضبط قد يمتد إلى النظام المادي كله بما يتضمنه من معطيات وبرامج.

دور المتخصص في تفتيش أجهزة الحاسب الآلي :

للمتخصص الفني الذي يستعين به رجل الأمن دور مهم في التفتيش لضبط الجرائم المعلوماتية والمعلومات المحظورة ، كما في مجال الجرائم الإرهابية ، والمقصود هنا بكلمة المحظورة : تلك المعلومات ذات الصلة بتنفيذ جرائم إرهابية ، كما هو الحال بالنسبة

للمعلومات الإرشادية بشأن إعداد وتصميم قنابل بدائية تستخدم في التفجيرات ، وقد تكــون معلومات لها علاقة بمواعيد وأماكن تنفيذ بعض الجرائم ، مثل القتل والسرقة ...الخ.

يبدأ دور المتخصص هنا بدخوله المكان المراد تفتيشه بغرض الضبط ، حيث يقــوم بحفــظ جميع الملفات التي تسمى (كوكيز) ، وهي الملفات التي توضــح الاتصــال بــين الطرفين ، وذلك لتحديد مكان الطرف الآخر في الاتصال. بالإضافة إلى حفظ المواقع مــن الــ (History) الخاص بالجهاز وذلك لدراستها وتحديد ما إذا كانت من المواقع المحظــورة أمنياً أم لا ، ومن جانب آخر ، فإن محاولة تفتيش جميع أجزاء الجهاز الخاصــة بــالحفظ وهي وسائط الحفظ المختلفة الأشكال مثل (الفلاش ، والهارد ديسك ، الاسطوانات).

المطلب الرابع - شروط وعناصر التحقيق في الإجرام المعلوماتي:

من المقرر – والمعروف قانوناً – أن التحقيق في مجال جرائم تقنية المعلومات ، بل وفي الجرائم التقليدية ، يتطلب توافر عدة شروط أساسية ، تلخص فيما يلي :

1. أن يكون التحقيق جارياً بصدد جريمة (جناية أو جنحة).
2. أن تكون الجريمة قد وقعت فعلا ، أو ترجح وقوعها.
3. أن ينسب ارتكاب هذه الجريمة إلى متهم معين ، أو للبحث عن هذا المتهم.
4. أن تتخذ وسائل التحقيق لجمع الأدلة والكشف عن مرتكب الجريمة.

أولا – أن يجرى التحقيق بصدد جريمة (جناية أو جنحة) :

يجب أن توجد جريمة ، معاقب عليها في القانون ، فلا شأن للمحقق بعمل لا يشــكل جريمة. وأساس القول بوجود الجريمة – في الأصل – هو قانون العقوبــات الاتحــادي ، ويجرى التحقيق بشأن واقعة توصف بأنها جناية أو جنحة. فلا يجرى التحقيق في جريمــة تعد مخالفة ، ويكفي أن يتوافر في الجريمة محل التحقيق ركنها المادي المكون لها ، بغض النظر عن الركــن المعنوي لدى الجاني. لأن البحث في مسئولية الجاني عن الواقعة غيــر

المشروعة ، فيبحثها القاضي بمناسبة الدعوى الجزائية ، ويلزم أن تكون تلك الجريمة من جرائم تقنية الحاسوب والانترنت التي تناولها القانون رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات.

ثانيا – أن تكون الجريمة قد وقعت فعلا ، أو ترجح وقوعها:

العبرة في اتخاذ إجراءات التحقيق في شأن جرائم تقنية المعلومات أن تكون الجريمة محل التحقيق قد وقعت فعلا أو ترجح وقوعها. فلا يجرى التحقيق بشأن جريمة محتملة. وإلا كان الإجراء باطلا.

وفي هذا الصدد يثور التساؤل حول أمرين :

الأول: الإجراءات السابقة على مباشرة التحقيق ، والتي تجرى لكشف جريمة قد تم الإعداد أو التخطيط لارتكابها.

الثاني: إجراءات الضبط الإداري التي تتخذ للعمل على منع وقوع الجريمة.

مما لا شك فيه أن لمأمور الضبط القضائي أن يباشر إجراءات الاستدلال ، وجمع التحريات بشأن وجود دلائل كافية على وجود جريمة قامت الدلائل الكافية على وقوعها. كأن يأمر بالقبض على المتهم الحاضر الذي توجد دلائل كافية على ارتكابه جريمة في الجنايات عموما دون تحديد لنوعها [1].

كما أن التحري والاستدلال بشأن الجرائم – تقليدية أم تقنية – من صميم عمل مأمور الضبط القضائي [2]. وقيام هذا الأخير بضبط جريمة في حالة تلبس بناء على هذه التحريات ، يكون صحيحا ، ولا يعتبر تحريضا على الجريمة [3].

1- في هذا المعنى حكم المحكمة الاتحادية العليا جلسة 2002/11/9 مج الأحكام س 24 رقم 169 ص 1108

2- في هذا المعنى اتحادية عليا جلسة 2004/5/3 مج الأحكام س 26 رقم 30 ص 298.

3- اتحادية عليا جلسة 2004/5/3 سالف الذكر.

وبالنسبة للموضوع الثاني ، فإن صدر قانون في إيطاليا ، أطلق عليه " قانون الجبر على منـــع الجريمة " ، مفاده أنه عندما تعلم الشرطة من خلال التحريات بأن هناك جريمة ســـوف ترتكب ، فإنه يتعين عليها العمل على منعها [1].

ثالثا – أن يجرى التحقيق في مواجهة متهم معين بارتكاب الجريمة ، أو للبحث عنه :

ويتطلب ذلك معرفة من هو المتهم بارتكاب الجريمة ، سواء كانت تقنية أم تقليدية ؟. ينصرف اصطلاح المتهم إلى الشخص الذي يوجه إليه الاتهام بارتكـــاب إحـــدى الجـــرائم المنصوص عليها في قانون العقوبات الاتحادي أو في أحد التشريعات الجنائية الخاصـــة ، كقانون مكافحة تقنية المعلومات ، سواء بوصفه فاعلا أم شريكا فيها [2].

وقد عرفت محكمة النقض المصرية المتهم بأنه " كل من وجه إليه الاتهام بارتكـــاب جريمة معينة ، ولو كان ذلك أثناء قيام مأموري الضبط القضائي بمهمة البحث عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم التحقيق والدعوى مادامت قد قامت حوله شـــبهة أن له ضلعا في ارتكاب الجريمة التي يقوم أولئك المأمورون بجمع الاستدلالات فيها " [3].

وقد تثبت صفة المتهم في فترة سابقة على رفع الدعوى. والقاعدة أن صفة المـــتهم تثبت للشخص عند توجيه الاتهام إليه من سلطات التحقيق ، ويمكن أن تثبت هـــذه الصـــفة كذلك باتهام يوجهه الأفراد في حالات الاتهام الخاص.

1- يتعلق هذا القانون بالتعامل مع رجال المافيا في إيطاليا.

2- محمد سامي النبراوي : استجواب المتهم ، رسالة دكتوراه ، القاهرة ســـنة 1968 ، ص 58 ــ ســـامي صادق الملا : اعتراف المتهم ، رسالة دكتوراه ، القاهرة سنة 1966 ص 26.

3- نقض 1966/11/28 مج الأحكام س 17 رقم 219 ص 1161.

رابعا – أن تتخذ وسائل التحقيق لجمع الأدلة والكشف عن مرتكب الجريمة :

تختلف صفة المتهم عن المشتبه فيه : فيوجد هذا الأخير عندما تكــون الشــبهات أو الأدلة من الضعف والبساطة ، بحيث لا يرجح معها الاتهام ، ويجب أن تنسب الجريمة إلى متهم معين. فإذا لم يعين تعيينا نافيا للجهالة ، فإن الاستدلالات والتحقيق تجريان للكشف عن شخصيته ، وينسب إلى المتهم ارتكاب الجريمة ، أي أن ينسب إليه مساهمته في ارتكابها ، سواء بصفته فاعلا أصليا أم مشاركا فيها.

خاتمة

يبدو من وجهة نظرنا أن المشكلات المثارة من خلال مكافحة جرائم تقنية المعلومات لن تجد لها حلاً في الوقت القريب ، والمسائل المستقبلية التي ينبغي توجيه النظر إليها هي المتعلقة بالتحليل العلمي لإساءة استخدام تكنولوجية تقنية المعلومات والانترنــت ومكافحتــه ولذلك فإن المأمول أن يتدخل المشرع ببعض التعديلات الإجرائية اللازمة في هذا الإطــار حيث أن النصوص الإجرائية التقليدية القائمة باتت غير ملائمة للتطبيق على جرائم تقنيــة المعلومات وحتى حدوث ذلك فإن الأمل أن يتبني الفقه والقضاء تفســيراً متطــوراً لهــذه النصوص وفي إطار من الشرعية الجنائية مع ضرورة تطور الأساليب الخاصــة بالبحــث والتحقيق في جرائم تقنية المعلومات الآن هذه الجريمة من الجرائم غير التقليدية ، ولذا يجب أن تجابه بأساليب بحث وتحر وضبط تحقيق غير تقليدية أيضا ، وفي هذا الإطار يتطلــب الأمر تدريب أجهزة إنفاذ وتطبيق القانون بأساليب الضبط وجمع الأدلة والتحقيق في جرائم تقنية المعلومات.

التوصيات

1- ضرورة تحديد الإجراءات الواجب اتباعها في ضبط وتحقيق جرائم تقنيـــة المعلومـــات وتقنية التحفظ على الأجهزة المستخدمة في ارتكاب هذه الجرائم وكيفية مقارنتها.

2- فيما يتصل بالأحكام الإجرائية ضرورة سن تشريعات واتخاذ التدابير الأخرى اللازمـــة لتحديد السلطات الضرورية والنظم الإجرائية لأغراض التحقيقات.

3- ما يتعلق بالتحفظ على بيانات الحاسب الآلي ضرورة سن تشريعات وطنية واتخاذ تدابير تمكن السلطات المختصة للأمر أو القيام بالتحفظ على البيانـــات المخزنـــة فـــي نظـــم الحاسوب.

4- فما يتعلق بأمر الإحضار ضرورة سن تشريعات وطنية واتخاذ تدابير تمكن الســـلطات المختصة من إصدار أمر إلى :

أ– أي شخص داخل الدولة بإحضار أية جهاز حاسب آلي أو أية بيانات مخزنـــة فـــي شبكات حاسب آلي في حيازته أو تحت إدارته.

ب– أي مقدم خدمات داخل الدولة. بإحضار المعلومات المتعلقة بالمشـــتركين لـــديها أو تحت إدارته.

5- بيان صيغ الاذن الصادر – من النيابة العامة لضبط هذه النوعية من الجرائم ودراســـة أوجه البطلان فيها ووضع ضوابط لصحة الإجراءات.

6- تامين البرامج المضبوطة قبل تشغيلها.

7- عقد دورات للقائمين على التحقيق في جرائم الحواسيب الآلية من أعضاء النيابة العامـــة وكذا القضاء لشرح هذه النوعية من الجرائم وإحاطتهم بكيفية التعامل معها.

المراجع

أولا - المراجع العربية :

1- دكتور. أحمد وهدان ، الانعكاسات الأمنية للعولمة ، القاهرة : المجلة الجنائية القومية ، مج 44 ، ع1 ، 2 ، مارس/يوليو 2001 ، ص91.

2- دكتور. أحمد وهدان ، تقييم فعاليات المواجهة التشريعية لجرائم الانترنت ، إمارة الشارقة ، مركز بحوث الشرطة ، مجلة الفكر الشرطي ، مج 13 ، عدد1 ، إبريل 2004 ، ص99.

3- اشرف صلاح الشيخ ، الجريمة المعلوماتية ، مجلة الأمن العام : القاهرة ، العدد 206 ، السنة51 ، يونيو 2009 ، ص117.

4- دكتور. حسني الجندي : التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة ، الكتاب الثالث. قانون مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة : الطبعة الأولى ، 2009.

5- دكتور. حسني الجندي : شرح قانون الإجراءات الجنائية ، الطبعة الرابعة ، دار النهضة العربية ، القاهرة ، 2004.

6- سامي حارب المنذري : موسوعة العلوم الجنائية ، تقنية الحصول على الآثار والأدلة المادية ، ج 1 ، بحوث الشرطة ، الشارقة ، الإمارات ط 1 سنة 2007.

7- سامي صادق الملا : اعتراف المتهم ، رسالة دكتوراه ، القاهرة سنة 1966.

8- سليمان أحمد محمد فضل. المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت) ، رسالة دكتوراه ، أكاديمية الشرطة ، القاهرة سنة 2007.

9- دكتور. عمر محمد أبوبكر بن يونس : الجرائم الناشئة عن استخدام الانترنت ، رسالة عين شمس سنة 2004.

10- دكتور. عمر السعيد رمضان : مبادئ قانون الإجراءات الجنائية ، القاهرة 1980 ، ج 1.

11- دكتور. عندليب الابراهيم : مقدمة في الكمبيوتر الشخصي : المقرر الثاني من رخصة قيادة الكمبيوتر الدولية ، شركة تقنية المعرفة ، ،2005.

12- دكتور. محمد أبو العلا عقيدة : التحقيق وجمع الأدلة في مجال الجرائم الالكترونية ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية ، دبي سنة 2003

13- دكتور. محمد أحمد الحمادي : تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات ، أحكام القضاء ، ضمن مجموعة البحوث الخاصة بالندوة العلمية التي نظمها مركز البحوث والدراسات الأمنية ، القيادة العامة لشرطة أبوظبي في الفترة من 6-7 نوفمبر سنة 2006م.

14- دكتور. محمد الأمين البشرى : التحقيق في جرائم تقنية المعلومات ، أكاديمية نايف ، 2002.

15- دكتور. محمد سامي النبراوي : استجواب المتهم ، رسالة دكتوراه ، القاهرة سنة 1968.
16- د. محمد السعيد ، الإرهاب الالكتروني ، القاهرة : مجلة الأمن العام ، العدد 206 ، السنة 51 ، يونيو 2009 ، ص97.
17- محمد علي عبيد الحمودي : دور مأمور الضبط القضائي في مواجهة جرائم المعلومات. [2000]
18- دكتور. محمد عيد الغريب : الاختصاص القضائي لمأمور الضبط القضــائي فــي الأحــوال العاديــة والاستثنائية ، سنة 2003.
19- دكتــور. مصطفى محمد موسى : دليل التحري عبر شبكة الانترنــت ، ســنة 2005 ، دار الكتــب القانونية ، المحلة الكبرى.
20- منير محمد الجنبيهي: أمن المعلومات الاليكترونية ، الإسكندرية : دار الفكر الجامعي ، 2006.
21- دكتور. نبيلة هبة هروال : الجوانب الإجرائية لجرائم تقنية المعلومات في مرحلة الاستدلال ، دراســة مقارنة ، الإسكندرية سنة 2007 ، دار الفكر الجامعي.
22- دكتور. هشام فريد رستم : الجرائم المعلوماتية ، القاهرة ، النسر الذهبي ، 2007.

ثانياً - هيئات ومؤسسات :

1- المحكمة الاتحادية العليا. دولة الإمارات العربية المتحدة.
2- موقع المباحث الفيدرالية الأمريكية (إف. بى. أى) ، وموقع وزارة الداخلية بجمهورية مصر العربيــة ، ومواقع الشرطة المحلية بدولة الإمارات العربية المتحــدة (الموقــع الالكترونــي .www. IFCCFBI (GOV).

ثالثاً - مراجع أجنبية :

1- Bouloc (Bernard) : L' acte d instruction , 1965 , No. 34 , p. 26 – Merle (Roger) – Vitu (Andre) : Traite de droit criminal , Procedure penale , 3 em. edition , Cujas 1979 m T. 2 em. , No. 1102 , p. 321.

رابعاً - مواقع أجنبية تقنية:

1- http://www2.its.strath.ac.uk/courses/pc-intro/
2- http://en.kioskea.net/contents/courrier-electronique/email-e-mail.php3
3- http://www.yale.edu/pclt/COMM/TCPIP.HTM
4- http://searchenterprisewan.techtarget.com/tip/Whats-in-a-packet-Bandwidth-utilization-series.

Investigation on IT Crimes [1]

Lt Colonel Dr. Sarhan Hassan Al Muaini [2]
Assist Lecturer of Police Sciences – Police Sciences Academy-UAE

Abstract

Unquestioningly, International Community is currently witnessing a stupendous tide of changes; or what is termed as Globalization. Raising the issue of IT Crimes comes in light of the emergence of a host of ideological and technological developments aimed at making the world a small village. However, the progress witnessed today in IT field has engendered a host of modern serious crimes which poses danger to law enforcement because of their international nature. Therefore, this study is intended to probe and figure out the various forms of one of these modern crimes which is IT crimes. The study defines IT Crimes and determines measures should be taken in investigation in addition to retaining devices used in the crime. Stomaching the subject from the hypothesis of efficiency of techniques used in combating IT Crimes, the study has adopted the analytical applied approach and tackled the issue via a number of key cores. Such cores are the various dimensions of IT Crimes, their features, characteristics and risks in addition to the techniques of investigation. Treatise arrives at the conclusion that combating efforts are infested with problems that defy solutions at least in the present time, and that attention should be directed to IT and internet misuse in an attempt to combat it. In its epilogue, the treatise recommends that UAE legislations have to introduce some procedural amendments regarding IT Crimes since old penal articles can no longer be applicable. Besides, researcher urges that jurisprudence and judiciary should try to lay down an interpretation for the penal articles associated such crimes.

Keywords: Information Technology – Information – related Crimes – Information Criminal – Examination- Inspection – Criminal Evidences – Technical Evidence – Information Investigation.

1-**Manuscript** was submitted in June 2011, refereed in July 2011 and approved for publication in September 2011.

2-**Biography:** Lt Colonel Dr. Sarhan attained his doctorate of Police Sciences in 2005, and he is currently holding the position of Director of Police Sciences Academy in Sharjah – UAE. He presides over a number of Committees. He published a host of studies and participated in local and international conferences.